Multiplying and Dividing on a Spreadsheet

Suppose we have a coding polynomial, p(x) and we want to make a spread-sheet in which

1. we can enter an arbitrary message, described by bits
2. it will output the product of that message, considered as a polynomial, multiplied by p(x).

To be precise, suppose we enter out message in column B starting at row 11,

We want the product of that message and p(x) to appear in column C, starting at row 11

We can accomplish this by putting an appropriate entry in cell C11 and copying it down column C as far as appropriate (or further, extra doesn't matter)

How far is appropriate?

The number of cells from C11 to where you stop should be the number of bits in your code words.

So what goes in C11?

We illustrate this by an example. Suppose p(x) is $1 + x^2 + x^5$

This means a message bit in position B11 should produce (mod 2) a 1 in B11, in B13 and in B16.

And in General:?

The power of x for each monomial in the coding polynomial tells how far down the column from the message bit you put the corresponding coding bit.

To encode this we have to look at these facts from the point of view of the coding bits rather than the message bits. We have to answer the question: which message bits contribute to a given code bit?

The answer to this question is that for each monomial in p(x), its power tells how far back in the message column you have to look to see if it contributes.

Thus in our example $(1+x^2+x^5)$, the appropriate entry in cell C15 (for example) should be: =mod(B15+B13+B10,2).

So to encode, all you need to do here is to enter =mod(B11+B9+B6,2) into cell C11, and copy it down column C.

For any encoding polynomial there will be a term in what you put in C11 for each monomial in the coding polynomial, and the B cell referred to will be 11 less the power of the monomial.

Warning: when you do this, the spreadsheet will look at the non-existent message information in cells B6-B10. For our purposes the fact that the message has no such bits means we want the spreadsheet to take their contents to be 0's. To do so, however, it must not think there are non-numerical words in these cells. If it thinks that it will put nasty comments into the cells instead of the answers you want. You can cure this, if it happens by explicitly putting 0's in B6-B10.

Here is what the spreadsheet might look like for $p(x)=1+x+x^3$

Message in next column	1	=MOD(B11+B10+B8,2)
	0	=MOD(B12+B11+B9,2)
	1	=MOD(B13+B12+B10,2)
	1	=MOD(B14+B13+B11,2)
		=MOD(B15+B14+B12,2)
		=MOD(B16+B15+B13,2)
		=MOD(B17+B16+B14,2)

.

Dividing by a Polynomial on a Spreadsheet.

Dividing one polynomial by another is exactly like long division.

And here is how it goes. You will recognize this from your elementary school experiences. But it is much easier here than what you remember because the only numbers are 0 and 1 and addition is mod 2. There are no nasty 6's and 7's,

First you look at the leading bit of the thing you are dividing – (I think that thing is called the dividend) If the dividend is shorter by 1 or more in length than the divisor, you stop. Otherwise if that bit is a 0 you record a 0 in your quotient and shift your attention to the next bit. If your bit is a 1, you subtract (in our case adding is

the same as subtracting) the dividend from the divisor so as to change the leading bit to a 0, record a 1 in the quotient and shift your attention to the next leading bit.

So there are actually two steps involved: one is shifting to the next bit of the dividend and recording its leading bit. This you do for each leading bit. The second step is adding the divisor to the dividend if the leading bit of the dividend is 1.

This can be implemented on the spreadsheet with two instructions and copying. If the dividend has length q, the process will take up a q by q+1 rectangle, but so what?

There is another subtle advantage this has over ordinary long division. In the ordinary case you start with the most significant bit. Here you can start at either end (Think of it this way: if x=2 the most significant bit is at the high power end. If x=1/2, it is at the low power end. So you must be able to choose the "leading bit" at your favorite end and you are not confined to any particular one.)

Suppose your dividend is located in column E with leading bit in E11. Then put your divisor polynomial in column D starting with row 10, i.e., with leading bit in D10.

The first step
in dividing is to put =E11 into F10, and to copy that down as far as the next to bottom row of the dividend, and across the same number of columns to the right as one more than the difference in number of bits of the dividend and divisor.

This will implement dividing by 1. The bits on row 10 starting with F10 will be the dividend itself at this stage, written horizontally instead of vertically.

The second step: Enter into F11 the instruction: =mod(E12+F$10*$D11,2),

and copy that down and to the right,

How far down?

Until the last 1 in column D, which has the divisor

How far across?

This should go into all rightward columns with instructions here already in them.

What does this do?

If the current leading bit (what was in E11 and has been put in F10) is a 1 this adds the shifted bit of the polynomial p (which is in D11 because we built the shift in by having p start in D10) to the shifted bit of E

which is in E12)

Shouldn't we do this with row 10 as well?

If we wanted to make row 10 a row of 0's we would apply the second step to row 10 as well as to the rows beneath it. Not doing so means that row 10 will contain the quotient we want. Notice that the divisor and dividends were columns, and the quotient will appear in row 10, starting with column F,

Here is an example of the resulting spreadsheet, again with $p=1+x+x^3$ and a random word as dividend, smallest power first. The top row seen is row 10.

1		=E11	=F11	=G11	=H11
1	1	=MOD(F$10*$D11+E12,2)	=MOD(G$10*$D11+F12,2)	=MOD(H$10*$D11+G12,2)	=MOD(I$10*$D11+H12,2)
0	0	=MOD(F$10*$D12+E13,2)	=MOD(G$10*$D12+F13,2)	=MOD(H$10*$D12+G13,2)	=MOD(I$10*$D12+H13,2)
1	1	=MOD(F$10*$D13+E14,2)	=MOD(G$10*$D13+F14,2)	=MOD(H$10*$D13+G14,2)	=MOD(I$10*$D13+H14,2)
	1	=E15	=F15	=G15	=H15
	0	=E16	=F16	=G16	=H16
	1	=E17	=F17	=G17	=H17

Any other divisor and dividend can be handled similarly, with the same instructions and more copying.

What happens if there is a remainder? In other words if the dividend is not divisible by the divisor?

If there is no remainder, the entries in the last column should all be 0's. If not there is a remainder, and the dividend was not divisible by the divisor.

Is what is in the last column the remainder?

It will be if code and polynomial were arranged with highest powers first. Then when the divisor first becomes shorter than the last column, what would appear there would be the remainder, highest powers first.

I habitually do division by making the lowest powers the most significant ones. In that case what appears in those columns is not the remainder, but is closely related to it. Can you figure out how?